User protection in cyberspace. Some recommendations

Salaun, Anne; Louveaux, Sophie; Poullet, Yves

Published in:
Info

Publication date:
1999

Document Version
Publisher's PDF, also known as Version of record

Camford | info vol.1 no.6 december.1999 | the journal of policy, regulation and strategy for telecommunications information and media

 1463-6697/99/060521-17

article:

user protection in cyberspace some recommendations

Sophie Louveaux, Anne Salaün and Yves Poullet

This article makes recommendations for user protection in cyberspace. The recommendations relate to commercial communications, to the relationship between the service provider and the consumer, and to data protection. They aim at providing trust and confidence in electronic commerce. To this end, the paper also develops site labelling and alternative dispute resolution mechanisms as an answer to the internet user's interest in taking advantage of network technologies.

Sophie Louveaux is Assistant at the Law Faculty and Researcher at Centre de Recherches Informatique et Droit (CRID), Rempart de la Vierge 5, 5000 Namur, Belgium (Tel: +32 81 72 47 72; fax: +32 81 72 52 02; email: sophie.louveaux@fundp.ac.be).

Yves Poullet is Law Professor and Director of the CRID (Tel: +32 81 72 47 79; fax: +32 81 72 52 02; email: yves.poullet@fundp.ac.be).

Anne Salaün is Researcher at CRID (Tel: +32 81 72 52 05; fax: +32 81 72 52 02; email: anne.salaun@fundp.ac.be).

This article is the result of research in the field of user protection as developed in the framework of the E-CLIP project (Electronic Commerce Legal Issues Platform – ESPRIT Project DG XIII – http://www.jura.uni-muenster.de/eclip).

Electronic commerce is challenging the rules that provide protection for consumers, with regard to commercial communications and contracts concluded at a distance. New questions are arising as to the applicability and effectiveness of traditional rules in the on-line environment. The digital marketplace makes new difficulties emerge, confronting consumers with a new range of specific problems.

The situation of on-line consumers – namely consumers purchasing goods or services on the internet – could be significantly improved through the adoption of measures aimed at a better incorporation of the interests of internet consumers.

Following are a series of recommendations taken from various European legal instruments which correspond to the different steps of an electronic transaction, from the start of the commercial transaction to the actual resolution of potential disputes through the use of alternative dispute mechanisms.

Recommendations on user protection

The recommendations presented below relate to commercial communications, to the relationship between the service provider and the consumer and to data protection.

Commercial communications

A new form of commercial communication is being developed with the use of email addresses. This gives rise to 'spamming', namely the frequent and massive sending of commercial messages through the email boxes of consumers, leading to connection and downloading costs born by consumers.

A right to oppose the receipt of messages for commercial purpose is admitted in three European Directives:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of those data:[1] article 14-b urges Member States to grant the data subject with the right 'to object, free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing';
- Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunication sector[2] states that unsolicited calls for purposes of direct marketing should not be allowed either without the consent of the subscriber concerned, or in respect of subscribers who do not wish to receive such calls (article 12); and
- Directive 97/7/EC on the protection of consumers in respect of distance contracts:[3] article 10 § 2 recognizes the opt-out principle where individual distance communications may be used only where there is no clear objection from the consumer.

The effectiveness of a right of opposition presumes, however, the existence of a mechanism which allows consumers to make known to providers their position regarding unsolicited commercial communications. Information on such opposition mechanisms is required. First of all, consumers should be provided with information on the existence of such mechanisms. Article 14-b of Directive 95/46/EC explicitly provides for the Member states to take the necessary measures to ensure that data subjects are aware of this right of opposition.

1. *OJ*, 23 November 1995, L 281/31.
2. *Op cit*, 30 January 1995, L 24/2
3. *Op cit*, 4 January 1997, L 144

Practically, the opposition mechanism could materialize in two different ways:

- The first commercial communication sent to the consumer could contain information on the possibility of refusing to receive such messages, and on the steps to take in order to do so. In this first hypothesis, the duty to inform the consumer would rely on the author of the communication; or
- When the email address is granted, the access provider would inform the consumer on the right to oppose unsolicited commercial communications received via the consumer's email address. The duty of information falls here on the internet Access Provider. On request of the consumer to oppose himself to the receipt of commercial emails, the IAP would filter such messages as soon as they arrive in the IAP mailbox. This would prevent the consumer from receiving those messages, the costs of receipt and downloading thus being avoided.

Another alternative is the idea of 'suppression markers in internet addresses' as developed by the UK Data Protection Registrar. Through the use of this device, individuals could indicate their objection to have data about them collected or to receive unsolicited emails as a result of the visit of certain websites or the participation of certain groups. The duty to respect the consumer's preferences lies with the sender of the unsolicited messages.

The above-mentioned distinction concerns solely the information of the consumer on the opposition mechanism and on the consumer's right to subscribe to a list to be removed from commercial communications. Another step is the *concrete functioning of the list*: the question remains as to the monitoring of the list by a specialized body. Should it be a public body? Or a professional body gathering different categories of providers? Whatever the choice is, it should at least avoid a situation where an increasing number of opposition lists are proposed to consumers. This would certainly weaken their purpose.

It is recommended that the opposition mechanism should be centralized and should enable providers, before sending any message, to have access to email lists where the wish of the consumer to oppose the receipt of commercial communications has been clearly stated, and then to complete the list if they are aware of an opposition.

The user could take the initiative of registering his/her preferences not to receive unsolicited email messages by notifying the data protection authority. This notification would create a presumption of the knowledge of such an opposition by any sender of unsolicited messages. However this system implies that the data protection authority provides easy access to the list of persons who have opted out to those who intend to use the internet for commercial marketing. This is not, however, an easy task if one considers the global character of the internet. Moreover, the existence of opposition lists should match with consumers' wishes. The list should offer enough opposition means (ie opposition to all type of commercial communications; selected opposition to identified providers or to categories of providers, etc). The finality of the list should not be diverted and the contents of the list should not be re-used for commercial purposes.

The possibility of filtering commercial communications should be read in accordance with the Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market.[4] Article 7 states that an unsolicited commercial communication by electronic mail should be 'clearly and unequivocally identifiable as soon as the recipient receives it'. With such a principle, how would consumers be able to filter a commercial message before it arrives in their mailbox? Article 7 could have been better drafted by stating that a commercial communication should be identifiable as soon as the service provider sends it. Such a wording would have opened the possibility to offer filter services by allowing an identification of the commercial aim of the message as soon as it is sent. A third party would have been able to filter the messages on behalf of the consumer; the commercial communications would have been stopped before reaching the recipient's mailbox.

4. 18 November 1998, http://www.ispo.cec.be/ecommerce/legal.htm

This last solution of electronic agents filtering the messages previously identified as commercial communications, is the most appropriate as regards privacy concerns. Contrary to the other solutions, the receiver does not need to openly disclose their choice not to be subject to such communications, choice which in itself could be considered as sensitive information.

Furthermore, as a protection against the spamming of websites, the internet website provider may offer a possibility not to be indexed by search engines so as to prevent the reception of unsolicited advertisements on the website. This idea of a 'non robot' marker placed on the front page of the website has been promoted by the 'International Working Group on Telecommunications and Privacy' (Hong-Kong Session 1997) and is in the same line of thought as the right of individuals not to be victims of search engines through notification to a specific data base.

Identification of the service provider

Consumers are faced with the difficulty of establishing the identity and location of the provider with whom they deal, although such information ensures confidence and trust in the consumer's mind. There is a big difference with traditional commerce where the businesses the consumers contract with are easily identifiable and whose reputation is clearly established. Furthermore, the identification of the provider is all the more important in an international environment.

The identification of the service provider is requested by the proposal directive on e-commerce and the Distance contracts directive. In so far as the service provider is processing personal data[5] concerning the consumer, articles 10 and 11 of Directive 95/46/EC also require that the service provider identify themself as the controller of the processing and that they also provide information about the purposes of the processing and the different categories of recipients authorized to use the data.[6]

Apart from the information foreseen in those three Directives, one could also imagine a hyperlink with the site of such an official trade register or data protection authority that would allow direct consultation:

- whenever the provider holds a digital signature, a Certification Authority has issued a certificate. This certificate would easily identify the provider: as the certificate is public, a link could be offered to the Certification Authority's site;
- the labelling of the site would also allow consumers to check the identity of the website owner;
- a link could also be offered with the data protection authority that detains the register of processing operations and information concerning the controller of such operations (article 21 of directive 95/46/EC).

5. By 'processing of personal data', article 2 of the directive understands 'any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'. 'Personal data' shall mean 'any information relating to an identified or identifiable person' (article 2.a).
6. See 1.3.2.3. 'Transparency'

Information provided to the consumer

According to article 4 of the Distance Contracts Directive, the information to be given to the consumer must be provided 'in a clear and comprehensible manner in any way appropriate to the means of distance communication used'.

This should be understood as the forbidding of providers to make a distinction between categories of information by presenting a first range of information in an attractive way (use of colours, animated pictures, etc) and another range of information in an unattractive way aimed at dissuading consumers from reading them. The possibilities offered by the technique should not lead providers to hide some information to the detriment of others, thus misleading consumers by dissuading them from reading the whole range of information.

Furthermore, it is important to note that any information given prior to the transaction should be accessible at any step of the visit on the site: too often the information is no longer accessible once the good has been put in the 'shopping basket', even though it is important to enable the purchaser to come back to it. A link or an icon should allow a consultation of the product's information at any step of the transaction.

There is, therefore, a need to strengthen the information's content. This strengthening could be ensured by providing additional information to the consumer as well as a sample, and by complying with a transparency obligation.

Additional information

The information disclosed by the provider to the consumer prior to the conclusion of the contract is of crucial importance since the parties are not by nature in contact with each other. This statement is strengthened by the global environment of the network – where the exercise of the right of withdrawal takes a new dimension in terms, among others, of return costs – and by the interactivity of the network where numeric goods and software directly downloaded on the consumer's computer often fall under an exception to the right of withdrawal.

Article 4 of the Distance Contracts Directive enumerates a list of prior information provided to the consumer that should be understood as a minimum in the on-line environment: when the good ordered is 'immediately consumed' – in other words when it is directly downloaded on his computer – additional information should be granted to the consumer. Such information must enable the consumer to check the compatibility with his own software, in order to avoid technical incompatibilities: a situation where goods received on-line are not useable for incompatibility reasons due to a lack of prior information, would be unbearable for consumers, leaving them with a software they can neither exploit nor return.

Sample

Where the technology permits, a sample of the product should be sent to the consumer: we assume that for many products or software delivered on-line the sending of a sample, or in other words an indicative piece of the product, would not represent any technical difficulties for the provider. This would on the contrary have the advantage of placing potential purchasers in a context of confidence since they would be able to receive, free of charge, a sample of the digitized good they would have been reluctant to buy without this prior check. After receipt, the recipient would feel confident in ordering the good if it is in accordance with the characteristics described in the offer and technically compatible with the recipient's own system.

Transparency

The use of the internet to carry out transactions very often implies an invasion of privacy by the use of processing operations on personal data in a way that is invisible to the data subject. The data subject does not know about the processing and has no freedom to decide on it. The lack of transparency concerns not only the use of invisible processing tools (such as automatic hyperlinks to third parties, active content and 'cookies' mechanisms which are placed on the browsers), but also a lack of transparency as regards the risks presented by the use of internet, the different actors involved in the actual transmission of the data from the consumer to the final service provider and finally a lack of transparency as regards the transfer of personal data to countries which fall outside the scope of protection afforded by the European Directives (transborder data flows).

As regards the use of invisible processing tools, Recommendation 1/99 on Invisible and Automatic Processing of Personal data on the internet Performed by Hardware and Software,[7] recommends that the data subject is informed and thus made aware of the processing in question and that internet software and hardware products should provide internet users with information about the data they intend to collect, store and transmit and the purpose for which they are necessary and, if necessary, the fact that the data collection will take place outside Europe.

As concerns the risks presented by the use of internet, Recommendation N¡ R (99) 5 of the Committee of Ministers to Member States for the protection of privacy on the internet,[8] offers as a guideline to the internet service providers that they should inform users of privacy risks presented by the use of internet before they subscribe or start using the services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of data.

As for the transparency in the routing of the data, articles 10 and 11 of Directive 95/46/EC require that the data subject be informed of the identity of the recipients of the data 'in so far as such information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject'. If the 'recipients' are defined as those to whom the data are disclosed (see article 2.g), fair processing implies a maximum of transparency as regards the data subject. If it is therefore not absolutely essential to inform the data subject of all the persons involved in the routing of the message, even if they could possibly access personal data (hubs…), an obligation to do so could arise if there exists a possible threat that the data be reused by such intermediaries or transmitted by them to third parties liable to make wrongful use of such data (cyber-marketeers, for example).

It is therefore recommended that intermediaries in the routing of the message must be identified if they can access personal data and that a risk of invasion of the consumer's privacy exists. This is even more the case in the event that the data is transferred to countries outside the scope of protection afforded by the European Directives. This recommendation is in line with the recitals of the directive which provide in §47 that 'where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services'.

A question arises as to whether the obligation to be identified must be imposed on all service providers. Undoubtedly, this obligation must exist when the service offered is of a commercial nature or broadly offered against any remuneration; this is for consumer protection reasons. With certain other services such as journalistic information, ideological or political expression, the question is more controversial. Must we admit a certain right to

7. Adopted by the Working Party of article 29 of the data protection directive on 23 February 1999.
8. Adopted by the Committee of Ministers on 23 February 1999.

anonymity in order to protect the freedom of expression? It can be imagined that in cases of fear of pressure, certain people will be reluctant to sign the information they put on their website. The so-called 'Estelle Hallyday' case was interesting in that respect in so far as the information provider was anonymous and that the host provider refused to disclose their name.[9]

Perhaps a good balance would be that anonymity is a right but that this right may not be invoked in the case of a complaint against the website. In other words, the hosting service has the duty to reveal the identity of the Web server in the case of a legal action against them.

To sum up, the following information must be given to internet users:

• *First*, on the identification of the service provider:

	Identification of the service provider
Distance contract Directive *(article 4 Prior information)*	– the identity of the supplier and, in case of contracts requiring payment in advance, his address.
Privacy Directive *(articles 10 and 11)*	– the identity of the controller and of his representative if any.
Proposal on e-commerce *(article 5 General information to be provided)*	– name of the service provider; the address at which the service provider is established; – the coordinates of the service provider including his email address which allow for him to be contacted rapidly and communicate with in a direct and effective manner; – where the service provider is registered in a trade register, the trade register in which he is entered and his registration number; – where the activity of the service provider is subjected to an authorization scheme, the activities covered by the authorization and the coordinates of the authority providing this authorization; – for the regulated professions, the coordinates of the professional body where the service provider is registered, the professional title granted in the Member State of establishment as well as the applicable professional rules; – the VAT number.

• *Second*, another range of information should be disclosed to internet users:

	Other information
Distance contract Directive *(articles 4 and 5)*	*Article 4: prior information (before the contract is concluded)* – the main characteristics of the goods or services, – the price of the goods or services including all taxes, – delivery costs, where appropriate, – the arrangements for payment, delivery or performance, – the existence of a right of withdrawal, – the cost of using the means of distance communication, where it is calculated other than at the basic rate, – the period for which the offer or the price remains valid, – where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

9. http://www.droit-technologie.org/2_1.asp?actu_id=920142062&month=2&year=1999

	Other information (continued)
Distance contract Directive *(articles 4 and 5)* (continued)	*Article 5: confirmation of information (once the contract is concluded)* – written information on the conditions and procedures for exercising the right of withdrawal, – the geographical address of the place of business of the supplier to which the consumer may address any complaints, – information of after-sales services and guarantees which exist, – the conditions for cancelling the contract, where it is of unspecified duration or of a duration exceeding one year.
Privacy Directive *(articles 10 and 11)*	– the purposes of the processing for which the data are intended; – Any information in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject (such as the recipients or categories of recipients of the data, whether replies to questions are obligatory or voluntary, as well as the possible consequences of a failure to reply, the existence of a right of access and the right to rectify the data concerning the subject)
Proposal on e-commerce *(articles 6 and 10)*	*Article 6: commercial communications* – information on the commercial nature of the communication, – information on identity of the natural or legal person on whose behalf the commercial communication is made, – information on promotional offers (discounts, premiums, gifts) and on the conditions which must be met to receive them, – information on promotional competitions or games and on the conditions for participation. *Article 10: electronic contracts* – information on the manner of the formation of the contract by electronic means, notably the different stages to follow to conclude the contract, whether or not the contract will be archived, any existing means to correct handling errors; – information on the codes of conduct to which the service provider subscribes.

As far as the confirmation of information is concerned, the Distance Contracts Directive provides for the obligation to confirm the prior information given to the consumer. Article 5 states that 'the consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the prior information, in good time during the performance of the contract'. The term of durable medium implicitly refers to electronic distance contracts where a written document is not foreseeable: one cannot expect to receive a confirmation on paper in the frame of on-line contracts. One should not lose sight of the Directive's requirement: the consumer must 'receive' confirmation: the obligation rests on the provider, the consumer needs not play an active role. For example, the confirmation would not be satisfactorily validated if the provider simply contents himself with posting it on-screen and leaving the consumer the trouble of downloading or printing out the information.

A second important issue linked to the confirmation concerns the medium: to answer to the requirement that the medium is 'available and accessible' to the consumer, a choice should be given to them as to the medium used. Indeed, a confirmation could be available to the consumer but could not be accessible if the medium is not readable by their computer (eg a floppy disk where the file is saved in a different format). The issue of confirmation takes a new dimension since here again the compatibility between the provider's and the consumer's computer has important consequences: this situation finds no echo in traditional distance contracting where the confirmation is mostly sent through postal services, and no question of compatibility arises. It is therefore important that a choice is proposed to the consumer as to the medium through which the confirmation will be sent, taking into account the consumer's technical equipment.

Most of the time, the confirmation will be sent through an email, which is the easiest, quickest and cheapest way to reach the consumer. However, email is not always a solution if the consumer has reached the provider from a public place (eg cyber-café): no personal address is attributed to him in this case. Still, if the contract has been concluded in compliance with the requirements of the Proposal for e-commerce, it means implicitly that the consumer has been able to interact with the service provider, irrespective of the existence of a personal email address. Then, it is foreseeable that the confirmation reaches the consumer through a public place's email address, provided the service provider makes sure that the consumer has effectively received it.

To summarize:

- the information should be presented in a clear and comprehensive way, the technique should not be used to hide other information;
- where appropriate, additional information should be provided, notably with regard to technical features, the routing of the message, invisible hyperlinks, the risks presented by the use of internet;
- where appropriate, a sample of the product should be sent before conclusion of the contract, allowing the consumer to check the compatibility of the product with his own system; and
- a choice should be given to the consumer as to the medium used for the confirmation; no positive step should be expected from the consumer; the medium used should be compatible with the consumer's computer.

Interactivity with the service provider

A direct contact with the service provider should be made possible: the provider should offer a hyperlink to consumers to enable them to contact him for any request of information or complaint.

The technology offers possibilities that should be used by professionals: an icon placed on the provider's site would offer a real interactivity, questions would receive direct answers and complaints could be easily addressed. The theory of 'mutual benefits' implies that the benefits that the provider gains from the use of electronic equipment for the collection of data and conclusion of the transaction, must equally be granted to the user, notably in order to exercise their right of complaint through the use of these same electronic means.

Summing up of the transaction

Apart from the great opportunities offered by electronic commerce, risks of wrongful use are inherent to the technique itself: no former means of communication had ever offered consumers the possibility to conclude contracts so fast, by a simple mouse click. This rapidity obviously implies risks of misuse and can lead to the formation of undesired contracts due to technological mistakes.

Seeing the consumer engaged in a contract after an error is not satisfactory. Still, the consent of the consumer has to be given explicitly in order to avoid contests on the existence of the contract. The solution could be to present a final summing up of the transaction before the consumer definitely engages himself in a contract.

A summing up of the transaction would have the advantage of presenting to the consumer a recapitulation of all his choices (characteristics of the goods/services chosen, price, delivery costs, arrangements for payment, performance, exercise of the right of withdrawal, etc). This summary, presented on a unique page, allows a visualization of the content of the contract the consumer is willing to conclude and, above all, enables the consumer to bring rectification and thus avoid mistakes due to a misuse of the technique. The consent is then given to the summing up of the transaction, meaning a clear and comprehensive summary of the content of the contract: such a practice brings an end to consumers' mistakes leading to undesired contracts.

Contract formation

Concerning the moment at which the contract is concluded, article 11 of the Proposal for a Directive on certain legal aspects of electronic commerce foresees three different steps before the contract is deemed concluded:

- the first step is – obviously - the recipient's acceptance, when the consumer demonstrates his wish to conclude the contract by sending a message to the provider;
- the second step is the acknowledgement of receipt of the provider sent to the consumer; and
- and the third one is the confirmation of the acknowledgement of receipt by the consumer.

From a consumer's point of view, the time of conclusion of the contract would have been more appropriately chosen when the confirmation is *sent by the consumer*, instead of when the confirmation is accessible to the provider. The time of conclusion chosen in the Proposal makes the risk of a non receipt of the message by the provider borne by the consumer, although the latter cannot be held responsible for a technical failure.

In order to guarantee a means to prove the transaction and its content, a *recording of the transaction* should be provided to the consumer by the provider. Such a record would be useful for both parties: it would testify the contract, its content, the time of conclusion, etc It could be sent to the consumer through a similar medium to the one used for the confirmation of information, and would present the advantage of focusing on those major elements of the contract that the parties could refer to in case of dispute. In order to guarantee the validity and integrity of the recording, electronic signatures could be used.

Consent of the consumer

A condition of the legitimate processing of the personal data is that the data subject is able to consent to the processing of his personal data for other purposes than those provided for by the law. This principle follows on from article 7 of the Directive 95/46/EC, which provides a list of criteria for making the processing of data legitimate. Article 8 provides for criteria which concern sensitive data.

The data subject's consent shall mean any freely given specific and informed indication of their wishes, by which the data subject signifies the agreement to personal data about them being processed. The consent to the processing of sensitive data must be 'explicit'. This consent could be given electronically if the provider ensures that the user has been informed of his right to withdraw his consent at any time, that the user can be identified and that the consent is recorded and cannot be modified.

Providers should not condition the access to electronic services to the consent of the user to certain processing of personal data, unless this data is necessary for the purpose of carrying out the services.[10]

Minimization of the data

At each step of an electronic commerce transaction, only the necessary data may be processed unless the data subject has given his consent to further data being processed.

Providers must design their technical and organizational systems with the aim of collecting, processing and using either no personal data at all or as little as possible. For example, browser software should, by default, be configured in such a way that only the minimum amount of information necessary for establishing the internet connection is processed.

As concerns client persistent information (that is to say information related to the consumer which remains longer than one session on the computer equipment), the configuration of internet hard- and software products should not by default, allow for the collecting, storing or sending of such information. internet hard- and software products should allow the data subject to freely decide about the processing of his/her personal data by offering user-friendly tools to filter the reception, storage or sending of such information following certain criteria.[11]

Anonymization

Where services are to be delivered electronically, service providers do not necessarily need to know at all times the precise identification of the user.

Technology must be made available that will provide individuals with a secure method of authorizing and authenticating transactions whilst at the same time minimizing the actual need for identification wherever possible. In this line, the German Teleservices Act states that the provider must offer the user anonymous use and payment of services or use and payment under a pseudonym to the extent that it is technically feasible

10. This recommendation stems directly from Directive 95/46/EC, which imposes a necessary link between the data collected, and the purpose of the processing.
11. This can be found in Recommendation 1/99 mentioned above.

and reasonable. Similarly the Recommendation N¡ R (99) 5 of the Committee of Ministers to Member States for the protection of privacy on the internet, offers as a guideline to internet service providers, that before accepting subscriptions and connecting users to the internet, they should inform them about the possibilities of accessing the internet anonymously and using its services and paying for them in an anonymous way (for example through the use of pre-paid cards).

Increasing the consumer's trust

Site labelling and ADR are both solutions aimed at providing trust and confidence in electronic commerce: they both provide for an answer to internet user's interests by taking advantage of the network technologies.

Site labelling

Site Labelling[12] – or labellization of websites – is the combination of technology and audit procedures with the aim of answering consumers' expectations with regard to electronic commerce. It is materialized by an audit procedure estimating the compliance of the site with provisions applying in the fields of consumer protection, identification of the provider, protection of privacy, security, etc, and the posting of a label on the provider's site.

It certifies the quality of the site and allows a consultation of the label's content through a hyperlink available from the site's Web page. The consumer is thus enabled to check the commitments of the site.

Site labelling should not be taken as a substitute for legal or extra-legal provisions: it should definitely be considered as a complement to legislative and/or auto-regulation actions.

Labellization provides an answer to both consumers and businesses' expectations in Electronic Commerce: trust and confidence are developed with the use of this technique. The posting of a label on screen is deemed as a sign of quality and places the consumer in a context of confidence. Its further objective is to develop e-commerce.

Some recommendations can be formulated with regard to site labelling:

Information of the consumer

The aim of Site Labelling is to increase consumer confidence and trust in Electronic Commerce, it is therefore crucial that consumers are properly informed and aware about this technique. The consumer should easily understand the existence of a label on a website's screen.

Proper informing of the consumer should be made possible through a hyperlink: a simple click on the label icon should place in front of the consumer all relevant, comprehensive and easily understandable information.

The information presented to the consumer should notably include:

- *relevant information on the labelling company*: name and address, main activities, contact person, involvement in labelling activities, etc;
- *criterion to grant the label*: legal basis, scope of application of the label (fields of law covered, eg consumer protection, privacy, etc), procedure to award the label, withdrawal in case of non compliance, protection against fraudulent use of the label, etc;
- *report about the website*: commitments to comply with the criterion developed by the labelling company.

12. See also Joseph Royen and Yves Poullet, Rapport AGORA 'Commerce électronique: vers la confiance!!

An interactive communication between the labelling company and the consumer should be made possible, enabling the consumer to make comments and ask questions. This information should be presented in a clear and comprehensive way, avoiding the reluctance of the consumer to read a huge quantity of information before understanding the meaning of labellization.

Quality of the labelling authority

The independence of the institutions in charge of site labelling is crucial in order to ensure confidence in the system. The efficiency of the control operated by these institutions is also important. Various remarks should be stressed:

Independence of the labelling authority

The independence might derive from the quality of the issuer of the label: public institutions or audit institutions. It might also be ensured through the procedure concerning both the definition of the criteria and the control of their compliance. Independence can be reached if the following conditions are met:

- the criteria are defined by a joint committee representing both consumers and website providers; and
- the same committee or another joint organ is involved in the control of the respect of the labelling conditions.

Furthermore, it is important that Web users are informed about the exact identity of the labelling authority as well as the procedure set up to grant the label and to ensure the compliance with the criteria.

Effectiveness of the control

As regard the effectiveness of the control, certain minimal requirements might be proposed:

- Firstly, the label ought to be delivered to a requester providing the existence of controlling measures and specific guarantees: commitment that the information given is true and complete; commitment that the label's criteria are complied with; commitment to refer to an ADR procedure, etc.
- Secondly, the duration of the label should be determined (a duration of 6 months seems appropriate);
- Thirdly, different mechanisms must be settled in order to check if a labelled site does comply with the fixed criteria. A *hot line* mechanism allowing each Web user to alert the appropriate authority in case of presumed non compliance should be recommended. Additionally, one might suggest the possibility for an independent cyber-tribunal to intervene as a 'mediator' or as an 'arbitrator' in case of litigation between a labelled website and a user. These 'alternative dispute resolution' mechanisms – ADR – are promoted by the Proposal for a Directive on certain legal aspects of electronic commerce.
- Fourthly, a certain awareness of the results of the control must be provided to the users. So, the publication of a 'black list', a report of the activities of the labelling authority or the ADR associated will be ensured.

Scope of application of a label

Given the international character of the internet, a label limited to the territory of a Member State would be a nonsense. Any initiative of labellization should at least focus on the European territory and on the European legislation, and should not lose sight of other initiatives – already existing or at the draft stage – at the international level.

A similar argument applies to the fields of law covered by the label: an

increasing number of labels placed on providers' sites would risk creating a deep confusion in the consumers' mind and risk damage to the provider's purpose and credibility.

It is quite clear, however, that a label focusing on a specific field of law or a specific activity would be better adapted than a general one, but the posting of a dozen labels on a single site, or a different label on each different site would be quite confusing.

Ideally, a balance should be reached between those two arguments in order to keep the interest of the label effective.

Minimal requirements

Labellization should not be heard as a compulsory standard for electronic providers. It should exist on a voluntary basis.

Labellization should not dedicate any monopoly, be it public or private. It should be based on a competitive market where any company is free to propose a labelling activity. Then, the setting-up of the label should be made in cooperation with professional associations involved in the setting-up of the label's criterion, eg consumer associations, professional associations of a particular sector, etc. Official authorities, although not be responsible for the initiatives of labellization, could be associated in the setting-up of criteria for the label. Such an involvement would help provide more credibility to the technique.

Security must be provided with regard to the use of the label:

- the label should not be reproducible by a non-authorized person, from both a technical and a legal point of view;
- the label should not be falsified; and
- the withdrawal of the label should be made possible only by the labelling company.

Costs are inevitably incurred by the labelling activity: audit performance, periodical checks, etc. The cost required by the labelling company should not be prohibitive for SMEs engaged in e-commerce.

The labelling company should not escape from its liability: it should be aware of its liability with regard to the label granted and the consequences. Whether for the audit report, the monitoring of the label, the relation with third parties or the consequences of non-authorized use, the labelling company should face its liability. In practice, it means that the company should take the necessary steps to be covered by a professional insurance for the possible damages. Likewise, the company in charge of auditing a site will be submitted to an obligation of secrecy applicable to all information collected at the occasion of the audit procedure.

Alternative disputes resolution mechanism: cyber-magistrate

Cyber-magistrate is a specific form of ADR, combining the technology and a mediation or an arbitration procedure, specially designed for electronic commerce operations.

The main idea is to provide to the Web users with an avenue for suing an information society service provider through electronic means in cases of alleged non-compliance with the regulatory requirements applicable to the electronic commerce transaction. (These could include non-respect by the service provider of the author's right of the complainant, non-delivery of the promised good, false advertising, illegitimate blocking of a website, etc.)

So required, the cyber-magistrate will act either as a *mediator*, or as an *arbitrator*. In the first case, the competence of the cyber-magistrate will be limited to search, with the parties involved in the litigation, a compromise satisfying the different parties. In the second case, the parties will acknowledge to the cyber-magistrate the competence to take a constraining decision that might be enforced by the official courts through the exequatur procedure.

Different experiences of ADR have been developed, mainly in North America.[13]

The cyber-magistrate should be seen as a way to provide more effectiveness as concerns the respect of the regulatory requirements in so far as:

- first, an easy and not costly access to the magistrate is provided through electronic means; and
- second, the cyber-magistrate has the possibility to use the electronic means (including, for example, video conference) in order both to communicate with the parties and to enforce his decision.

Finally, it might be expected that a more rapid solution would be offered in comparison with traditional public jurisdiction. It is also obvious that one might expect that only relevant specialists in electronic commerce would be proposed as cyber-magistrates.

The cyber-magistrate presents an attractive solution and numerous advantages, notably:

- its flexibility allows an adapted procedure and an adapted solution, within a limited period of time and at low-cost value;
- its confidential nature is also of importance for businesses who might prefer to see their conflicts solved without any publicity; and furthermore
- an alternative solution presents fewer difficulties with regard to the enforcement of the decision, compared to the difficult enforcement of a judicial decision, especially in an international environment.

According to article 17 of the Proposal for a Directive on certain legal aspects of Electronic Commerce, Member States shall ensure that, in the event of disputes between an information society provider and its recipient, their legislation allows the effective use of out-of-court settlement mechanisms including by appropriate electronic means. The conditions for such an alternative way to solve disputes are explained in paragraph 2: the bodies responsible for out-of-court settlement of disputes shall apply the principles of independence and transparency, the adversarial principle and the principles of effectiveness of procedure, legality of the decision, liberty of parties and representation.

As stated in the recitals of article 17, out-of-court dispute settlement should be 'particularly useful for some disputes on the internet because of their low transactional value and the size of the parties, who might otherwise be deterred from using legal procedures because of their cost'.

ADR is seen as a complement to judicial procedures, its aim is to propose a tailor-made solution better adapted to the particularities of the network than traditional court procedures. To be fully efficient and adapted to the needs of the actors of the internet, it is foreseen that an alternative way of solving disputes should comply with minimal requirements, such as a certain quality of the person in charge of solving the disputes, with a necessary condition of neutrality and independence; the transparency of the activities of the cyber-magistrate in order to benefit others; the necessarily voluntary character of the procedure; the proper information of the consumer about the purpose of the procedure; the compliance of the decisions adopted with the legal requirements notably as regards consumer protection; the complementarity with a traditional court role.

Furthermore, the complementarity with the technique of site labelling should not be ignored as both participate in the development of a context of confidence and trust on the internet.

13. Cybertribunal: http://www.cybertribunal.org
Online ombudsman Office: http://aaron.sbs.umass.edu/center/ombuds/default.htm
OMPI: http://www.arbiter.wipo.int/
WIPO On-Line Dispute Resolution Service for internet ONE: http://internetone.wipo.int/
Virtual Magistrate: http://vmag.vcilp.org/
IRIS – Mediation: http://www.iris.sgdg.org/mediation/index.html

Here again, some recommendations can be formulated with regard to ADR:

Quality and independence of the cyber-magistrate

The third party asked to solve the dispute should present a specific competence as regards electronic commerce and electronic transactions. The independence of this third party is also a crucial point: it should not represent the interests of a party to the detriment of the other.

In that sense, the university sphere might play an important role as it is the case presently in the first CyberTribunal experiments. The cyber-magistrate should be neutral and, as far as possible, be established at a local level in order to facilitate the contacts with local consumers and to avoid problems such as languages, culture, national habits, etc.

Moreover, certain existing rules about the arbitration and the designation of the arbitrators might be applicable.

Transparency of the activities

Transparency is expected regarding notably the following:

- the choice of the person acting as a cyber-magistrate;
- the method of work of the cyber-magistrate;
- the procedure to adopt the decisions;
- the constraining force of the decisions.

Likewise, the activities of the cyber-magistrate should, as far as possible, be transparent: the decisions adopted should be available on the site of the cyber-magistrate, while guaranteeing the anonymity of the persons involved in the procedure. Such publications should allow actors of the internet to be aware of the disputes that arise between parties, and of the solution that was brought to the dispute.

Information of the consumer

Proper information for consumers on the technique of cyber-magistrate should be provided. It is of crucial importance that consumers properly understand the meaning and the purpose of the mechanism and of the interests it presents for the dispute.

The information provided should therefore concentrate on the mechanism of the cyber-magistrate, its functioning, the consequences for the parties involved in the procedure, the rights and obligations of each party, the constraining character or not of the decision, the compliance with the legal requirements, the possibility at any step of the procedure to stop the alternative procedure and go to court, etc.

This information should be aimed at enabling any consumer to understand the procedure and the steps to follow.

Voluntary character of the procedure

The choice of an alternative procedure to solve a dispute should be based on a totally free decision of both parties. No party should feel obliged to choose this way of solving disputes. This is the reason why the above-mentioned information takes a crucial importance, as the parties should be well aware of the non-compulsory character of the procedure. The option of each party should therefore be given freely, which implies that even if the parties have previously opted for an alternative solution, this does not preclude the parties from giving their consent again at the time the dispute arises and possibly changing their opinion.

This voluntary character also implies the possibility for both parties to withdraw from the procedure at any step, and to decide eventually to go to court.

Representation

The alternative procedure should also allow a representation of the parties, notably by professional bodies such as consumer associations, professional associations or federations. The representation by a lawyer should obviously also be possible.

Compliance with legal requirements

Existing legal requirements should be taken into account in the decision adopted by the cyber-magistrate. Such an alternative way to solve disputes should not be seen as a regulatory approach in itself where legal obligations are modified. It should, on the contrary, comply with the existing legislation in the fields of consumer protection, privacy protection, trade practices, etc.

This compliance will notably participate in increasing the credibility of the cyber-magistrate.

Complementary with traditional courts role

The initiative of cyber-magistrate should be complementary to traditional courts in so far as traditional means of dispute settlements should also be reachable through electronic means in the future. A positive influence should be exercised on the traditional procedure.

It is strongly recommended that the development of mechanisms of dispute resolution through the use of electronic means will be the fact not only of private initiatives but also of the public service of Justice in the context of the necessary modernization of the functioning of the traditional Courts. It seems that the possibility of Courts' seizure through electronic means ought to be enforced legally and that in case of trivial cases or cases of minor importance, the possibility of judging or sentencing by electronic means must exist. Moreover, the judge must have the competence to use the new techniques in order to communicate his sentence and to enforce it.

Conclusion

Besides the recommendations formulated with regard to user protection, whose aim is to provide a better protection, site labelling and ADR are both mechanisms aimed at providing trust and confidence. All together, such initiatives are a means of developing confidence in electronic commerce.

Site labelling and ADR materialise the wish of website owners to take into account the interests of Web users in order to increase exchanges between themselves. In other words, site labelling and ADR are answers provided by websites owners to the fears of users who might be reluctant to conclude contracts on the internet because of the uncertainty linked to this new form of doing business.

Likewise, ADR should be seen as a follow-up of site labelling in so far as the commitments taken by the site in the frame of the labelling process can be sanctioned (in case of non-compliance) by the possibility offered to the user to submit a dispute to an on-line magistrate. While site labelling is a first step towards the development of a context of confidence and trust, ADR is a second step attesting to the site's commitment to see possible infringements sanctioned through an on-line procedure adapted to the technique used.